## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

**Listing of Claims:**

Claim 1 (Currently Amended): A method for controlling access to a resource of a device, the method comprising:

storing, within a device, authorization data that defines at least one class of clients that access the device, wherein the authorization data defines for each class of clients: (i) an access control attribute that specifies coarse-grain access control rights for members of the class to configuration data for a resource provided by the device, and (ii) an associated regular expression specifying a textual pattern that specifies fine-grain access control rights for the members of the class to only a portion of the configuration data for the resource provided by the device;

receiving, with the device, a command from a client, wherein the command requests access to the portion of the configuration data for the resource of the device;

identifying the class of which the client is a member;

retrieving, from the authorization data, both the access control attribute and the regular expression for the identified class of which the client is a member;

evaluating the command using the retrieved regular expression to determine whether the command matches the textual pattern specified by the retrieved regular expression; and

controlling access to the portion of the configuration data requested by the client based on both: (i) the coarse-grain access control rights to the configuration data of the resource specified by the access control attribute for the identified class of which the client is a member, and (ii) the evaluation of the regular expression for that class,

wherein controlling access comprises allowing access to the configuration data when the access control attribute denies access to the resource and the textual pattern of the regular expression matches the command.

Claim 2 (Cancelled).

Claim 3 (Currently Amended): ~~The method of claim 1,~~

A method for controlling access to a resource of a device, the method comprising:

storing, within a device, authorization data that defines at least one class of clients that access the device, wherein the authorization data defines for each class of clients: (i) an access control attribute that specifies coarse-grain access control rights for members of the class to configuration data for a resource provided by the device, and (ii) an associated regular expression specifying a textual pattern that specifies fine-grain access control rights for the members of the class to only a portion of the configuration data for the resource provided by the device;

receiving, with the device, a command from a client, wherein the command requests access to the portion of the configuration data for the resource of the device;

identifying the class of which the client is a member;

retrieving, from the authorization data, both the access control attribute and the regular expression for the identified class of which the client is a member;

evaluating the command using the retrieved regular expression to determine whether the command matches the textual pattern specified by the retrieved regular expression; and

controlling access to the portion of the configuration data requested by the client based on both: (i) the coarse-grain access control rights to the configuration data of the resource specified by the access control attribute for the identified class of which the client is a member, and (ii) the evaluation of the regular expression for that class,

wherein controlling access comprises denying access to the configuration data when the access control attribute grants access to the resource and the textual pattern of the regular expression matches the command.

Claim 4 (Original): The method of claim 1, wherein storing authorization data comprises storing the authorization data as an authorization class that conforms to a class syntax.

Claim 5 (Cancelled).

Claim 6 (Previously Presented): The method of claim 1, wherein the coarse-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources within the network device.

Claim 7 (Previously Presented): The method of claim 1, further comprising receiving the command from the client via a command line interface.

Claim 8 (Original): The method of claim 7, wherein evaluating the command comprises evaluating the command in real-time while the client inputs the command via the command line interface.

Claim 9 (Currently Amended): A method comprising:

storing, within a device, configuration data for one or more resources provided by the device, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of higher-level objects and a plurality of lower-level objects, and each of the higher-level objects represents a portion of the configuration data that relates to a respective one of the resources of the device;

storing, within the device, authorization data that defines at least one class of clients that access the device, wherein the authorization data defines for each class of clients: (i) an access control attribute that specifies coarse-grain access control rights for members of the class to the configuration data for the resource, and (ii) an associated regular expression specifying a textual pattern that specifies fine-grain access control rights for the members of the class to only a portion of the configuration data for the resource;

receiving, with the device, a command from a client, wherein the command requests access to one or more of the lower-level objects of the configuration data for a particular one the resources of the device;

identifying the class of which the client is a member;

retrieving, from the authorization data, both the access control attribute and the regular expression for the identified class of which the client is a member;

evaluating the command using the retrieved regular expression to determine whether the command matches the textual pattern specified by the retrieved regular expression; and

controlling access to the one or more lower-level objects of the configuration data requested by the client based on both: (i) the coarse-grain access control rights for the higher-level object of the configuration data for the requested resource as specified by the access control attribute for the identified class of which the client is a member, and (ii) the evaluation of the regular expression for that class with respect to the requested one or more lower-level objects of the resource,

wherein controlling access comprises allowing access to the configuration data when the access control attribute denies access to the resource and the textual pattern of the regular expression matches the command.

Claim 10 (Original): The method of claim 9, wherein the objects have respective textual labels and the regular expression defines the textual pattern to match the textual labels of a set of one or more of the objects within the configuration hierarchy.

Claim 11 (Original): The method of claim 10, wherein evaluating the command comprises applying the regular expression to the command to determine whether the command specifies any of the objects within the set.

Claim 12 (Original): The method of claim 9, further comprising pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

Claim 13 (Previously Presented): The method of claim 9, further comprising pre-processing the regular expression so that the command is evaluated with the regular expression in real-time as the client enters the command.

Claim 14 (Original): The method of claim 13, wherein evaluating the command comprises evaluating the command with the pre-processed regular expression each time the client enters a token indicating a textual break within the command.

Claim 15 (Original): The method of claim 1, wherein controlling access comprises controlling access to configuration data of a router.

Claims 16–21 (Cancelled)

Claim 22 (Currently Amended): A computer-readable medium comprising instructions for causing a programmable processor to:

store, within a device, authorization data that defines at least one class of clients that access the device, wherein the authorization data defines for each class of clients an access control attribute and an associated regular expression defining a textual pattern, and further wherein the access control attribute is a coarse-grain access control attribute defining access control rights to a resource provided by the device and the regular expression defines fine-grain access control rights for members of the class to a portion of the resource provided by the device;

receive, with the device, the command from a client, wherein the command requests access to configuration data of the device;

identify the class of which the client is a member;

retrieve, from the authorization data, the access control attribute and the regular expression for the identified class of which the client is a member;

evaluate the command using the retrieved regular expression to determine whether the command matches the textual pattern specified by the retrieved regular expression; and

control access to the configuration data by the client based on the coarse-grain access control attribute for the identified class of which the client is a member and the evaluation of the regular expression for that class,

wherein the instructions cause the processor to allow access to the configuration data when the textual pattern of the regular expression matches the command.

Claim 23 (Cancelled).

Claim 24 (Currently Amended): A computer-readable medium comprising instructions for causing a programmable processor to:

store, within a device, authorization data that defines at least one class of clients that access the device, wherein the authorization data defines for each class of clients an access control attribute and an associated regular expression defining a textual pattern, and further wherein the access control attribute is a coarse-grain access control attribute defining access control rights to a resource provided by the device and the regular expression defines fine-grain access control rights for members of the class to a portion of the resource provided by the device;

receive, with the device, the command from a client, wherein the command requests access to configuration data of the device;

identify the class of which the client is a member;

retrieve, from the authorization data, the access control attribute and the regular expression for the identified class of which the client is a member;

evaluate the command using the retrieved regular expression to determine whether the command matches the textual pattern specified by the retrieved regular expression; and

control access to the configuration data by the client based on the coarse-grain access control attribute for the identified class of which the client is a member and the evaluation of the regular expression for that class,

~~The computer-readable medium of claim 22, further comprising~~ wherein the instructions ~~to~~ cause the programmable processor to deny access to the configuration data when the textual pattern of the regular expression matches the command.

Claim 25 (Cancelled).

Claim 26 (Previously Presented): The computer-readable medium of claim 22 , wherein the coarse-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources.

Claim 27 (Previously Presented): The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to receive the command from the client via a command line interface.

Claim 28 (Original): The computer-readable medium of claim 27, further comprising instructions to cause the programmable processor to evaluate the command in real-time while the client inputs the command via the command line interface.

Claim 29 (Original): The computer-readable medium of claim 22, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of objects, and each of the objects represents a portion of the configuration data that relates to one or more resources of the device.

Claim 30 (Original): The computer-readable medium of claim 29, wherein the objects have respective textual labels and the regular expression defines the textual pattern to match the textual labels of a set of one or more of the objects within the configuration hierarchy.

Claim 31 (Original): The computer-readable medium of claim 30, wherein further comprising instructions to cause the programmable processor to apply the regular expression to the command to determine whether the command specifies any of the objects within the set.

Claim 32 (Original): The computer-readable medium of claim 29, further comprising instructions to cause the programmable processor to pre-process the regular expression to automatically insert one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

Claim 33 (Original): The computer-readable medium of claim 29, further comprising instructions to cause the programmable processor to receive the command from a client via a command line interface, and pre-process the regular expression so that the command is evaluated with the regular expression in real-time as the client enters the command.

Claim 34 (Original): The computer-readable medium of claim 33, further comprising instructions to cause the programmable processor to evaluate the command with the pre-processed regular expression each time the client enters a token indicating a textual break within the command.

Claim 35 (Original): The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to control access to configuration data of a router.

Claims 36–55 (Cancelled).

Claim 56 (Previously Presented): The method of claim 1, wherein a resource is at least one of a present configuration of the device, policies and relationships with other devices, a configuration of an interface card of the device, a parameter for network protocols supported by the device, a specification for a physical component within the device, information maintained by the device, a software module executing on the device, device chassis inventory, device system parameters, routing policies, forwarding options, network flow statistics, error logs, user information, or performance metrics.